Overview

In order to support the Department's twenty four hour operations, employees need reliable access to databases, e-mail, file shares, web servers, and centralized applications. Due to the potential adverse impact on Department Systems and Department Networks, Department Computer Systems having the ability to use removable media (thumb drives, writable CDs, etc) must either have the removable media capability disabled - or that Department systems are configured to only use encrypted removable media.

Purpose

This document is intended to ensure that Department data are secure from inadvertent release and that Department systems are protected from potential threats deliverable via removable media. The potential adverse impact to Department operations and systems is so significant a threat - that only strong security measures can successfully prevent unsafe computer activity.

Audience

This document is for use by all Department of Crime Control and Public Safety personnel who use Computer systems.

Policy

The threat associated with removable media is fivefold: the first is that sensitive data on Department computers may easily be transferred outside the Department via removable media, the second is that removable media can be easily used as a malware attack vector to corrupt data on State computers (installed on the removable media), the third is that Department networks can be attacked or compromised via malware (from computers that execute malware originating from removable media), and the fourth is data store on such devices can easily be lost or stolen with minimal effort. Data stored on removable media that is lost or stolen can easily be accessed by non-Department computers.

Because removable media (thumb drives, CDs, etc) are often needed as a normal course of business of the Department, Department IT staff must apply the following measures to secure Department computer systems.

1. Systems are to be configured to ensure no applications can be stored or executed from the removable media. Only non-executable data is to be stored on removable media.
2. Department Computers should only have Department approved, legally licensed software installed - and such software can only be installed by Department system administration personnel (having appropriate system privileges).
3. All data stored on removable media (read or written) must be encrypted using Department, State, or Federally approved encryption software.

Enforcement

Exceptions to the above policy by written request only - and associated written granting authority - from either the Department Secretary, the Department CIO, the Agency/Division Head, or Department Designated Information Security Personnel. Any non-authorized effort to circumvent this policy is to be reported to the appropriate above individuals for further Federal, State, Department, or Agency personnel disciplinary action.

References

Statutory Authority: N.C.G.S. 147-33.110
Statewide Information Technology Standard: 050302
Organization for Standardization Standard: 27002 (ISO 27002)

Authorizing Signature(s)

Chief Deputy Secretary _____
Gerald Rudisill

Deputy Secretary _____
Jonathan S. Williams

Assistant Secretary _____
Rhonda Raney

Highway Patrol Commander _____
W. Fletcher Clay

Revision History

Draft 1 2 March 2007
Draft 2 5 March 2007
Draft 3 19 September 2007
Draft 4 10 October 2007